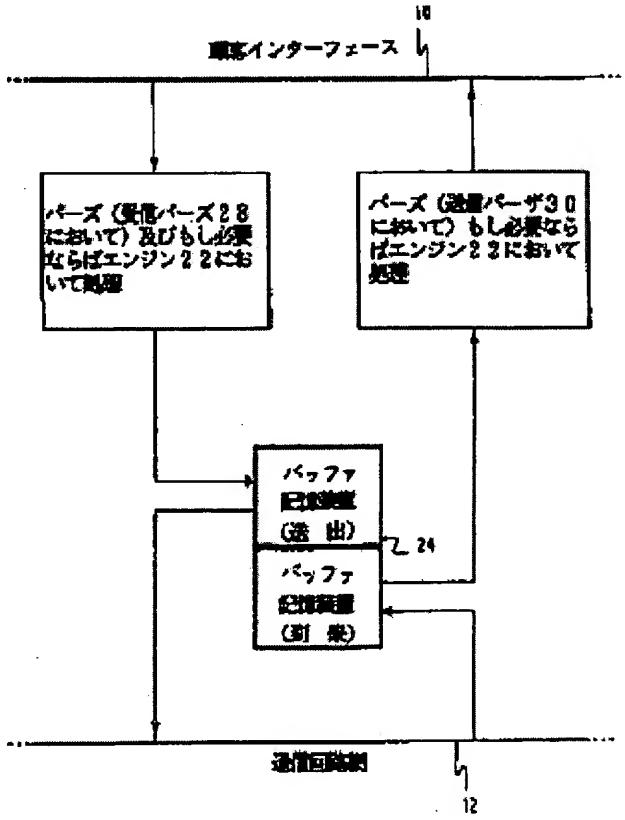
METHOD AND APPARATUS FOR PROCESSING CRYPTOGRAPH IN COMMUNICATION CIRCUIT NETWORK USING SINGLE CRYPTOGRAPHIC ENGINE

Patent number: JP5199220
Publication date: 1993-08-06
Inventor: FUIRITSUPU PINCHIYAAZU ROZOBUI; SHIIMAN TOBU BEN MAIKERU
Applicant: DIGITAL EQUIPMENT CORP
Classification:
- international: G09C1/00; H04L9/00; H04L9/10; H04L9/12
- european: H04L29/06
Application number: JP19920156793 19920616
Priority number(s): US19910722745 19910628

Also published as:
EP0525968 (A2)
EP0525968 (A3)

Abstract of **JP5199220**

PURPOSE: To provide a simple device which uses a single cipher engine to perform the cipher processing of data transferred between a customer interface and a communication circuit network bidirectionally. CONSTITUTION: An output data packet received from a customer interface 10 is immediately parsed by a means 28 to determine whether the cipher processing is requested or not; and if it is requested, a proper part of the packet is subjected to the cipher processing at the time of reception of the packet and is stored in a transmission buffer storage device 24 till transfered onto a communication circuit network 12. A data packet from the communication circuit network 12 is not immediately parsed, and it is stored in an arrival buffer storage device 24 until the customer interface is made available. Parsing and the required cipher processing of the arriving packet are not performed until the customer interface is made available and it is retrieved from the arrival buffer storage device for transfer. Only a single cipher engine is required for a half-duplex customer buffer.



Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平5－199220

(43)公開日　平成５年(1993) ８月６日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		9194－5L		
			7117－5K	Ｈ０４Ｌ　9／00　Ｚ	

審査請求　未請求　請求項の数15(全 11 頁)

(21)出願番号　特願平4－156793

(22)出願日　平成４年(1992) ６月16日

(31)優先権主張番号　０７／７２２７４５

(32)優先日　1991年６月28日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　590002873
ディジタル　イクイプメント　コーポレイション
アメリカ合衆国　マサチューセッツ州　01754メイナード　メイン　ストリート　146

(72)発明者　フィリップ　ピンチャーズ　ロゾヴィック
イスラエル　エルサレム　フランクフルテル　ストリート　2

(72)発明者　シーマン　トヴ　ベン　マイケル
イスラエル　ギラト　ゼール　ミッツペ　ストリート　1313

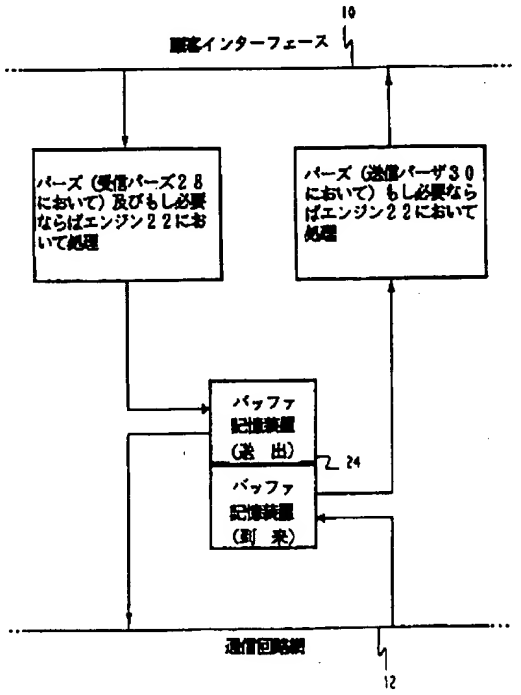
(74)代理人　弁理士　中村　稔　（外６名）

(54)【発明の名称】　単一の暗号エンジンを使用する通信回路網内の暗号処理方法及び装置

(57)【要約】　（修正有）

【目的】　“顧客”インタフェースと通信回路網間で両方向に転送されるデータを単一の暗号エンジンを使用して暗号処理する簡便な装置を提供する。

【構成】　顧客インタフェース１０から受信した出力データパケットは、暗号処理の要求の有無の決定のために直ちにパーズ２８され、要求されていればパケットを受信した時にその適切な部分が暗号処理され、通信回路網上へ転送されるまで送出バッファ記憶装置２４内に記憶される。通信回路網１２からのデータパケットは直ちにパーズされず、顧客インタフェースが使用可能になるまで到来バッファ記憶装置２４内に記憶される。到来パケットのパージング及び必要暗号処理は、顧客インタフェースが使用可能になり、転送のため到来バッファ記憶装置から検索されるまで遂行されない。半二重顧客バッファは単一の暗号エンジンだけが要求される。



1

【特許請求の範囲】

【請求項1】　半二重顧客インタフェースから通信回路網へ送出されるデータと、通信回路網から顧客インタフェースへ到来するデータとを暗号エンジン手段を使用して暗号処理する方法であって、

送出データパケットを顧客インタフェースから受信した時に、もし必要ならば、唯一の暗号エンジンを使用して暗号処理する段階と、

到来データパケットが顧客インタフェースへ送信されて来た時に、もし必要ならば、上記唯一の暗号エンジンを使用して暗号処理する段階と、

到来データパケットと送出データパケットとを転送する前に、必要に応じて、一時バッファ記憶装置内に記憶する段階と、

を具備し、顧客インタフェースが送出データパケットと到来データパケットとを同時に処理することができないために、単一の暗号エンジンだけしか必要としないことを特徴とする方法。

【請求項2】　処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各送出データパケットをパーズする段階と、

処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各到来データパケットをパーズする段階とをも具備する請求項1に記載の方法。

【請求項3】　到来パケットと送出パケットとを一時バッファ記憶装置内に記憶する段階が、

もし顧客インタフェースが使用不能であれば到来パケットを記憶する段階と、

もし通信回路網が使用不能であれば送出パケットを記憶する段階とを含む請求項1に記載の方法。

【請求項4】　ループバックパケットを顧客インタフェースから受信する段階と、

ループバックパケットを、もし必要ならば、直ちにパーズし、暗号処理する段階と、

もし顧客インタフェースが使用不能であればループバックパケットを記憶する段階とをも具備する請求項3に記載の方法。

【請求項5】　半二重顧客インタフェースから通信回路網へ送出されるデータと、通信回路網から顧客インタフェースへ到来するデータとを単一の暗号エンジンだけを使用して暗号処理する方法であって、

通信回路網から到来するデータパケットを受信する段階と、

受信した各パケット毎に顧客インタフェースが使用可能か否かを決定する段階と、

もし顧客インタフェースが使用不能であれば、顧客インタフェースが使用可能になるまで到来データパケットを記憶し、次いでそのパケットを検索する段階と、

データパケットを暗号処理すべきか否かを決定するため

2

にパーズし、もし必要ならば、単一の暗号エンジンを使用してそのパケットを暗号処理し、そのパケットを顧客インタフェースへ送信する段階と、

顧客インタフェースから送出されるデータパケットを受信する段階と、

顧客インタフェースから受信した各パケットをパーズする段階と、

もし先行パージング段階によって処理が必要であると決定されていれば、顧客インタフェースから受信した各パケット毎に上記単一の暗号エンジンを使用して暗号処理する段階と、

通信回路網が使用可能であるか否かを決定する段階と、

もし通信回路網が使用不能であれば、通信回路網が使用可能になるまで各送出データパケットを記憶し、次いでその送出パケットを検索する段階と、

送出データパケットを通信回路網上に送信する段階とを具備し、送出パケットの暗号処理をそれらのパケットが顧客インタフェースから受信した時に遂行し、また到来パケットの暗号処理をそれらのパケットが顧客インタフェースへ送信する時に処理するが、顧客インタフェースの半二重動作がこれらの両機能の同時発生の可能性を妨げるために、データの暗号処理の諸段階を遂行するには単一の暗号エンジンで十分であることを特徴とする方法。

【請求項6】　ループバックパケットを顧客インタフェースから受信する段階と、

ループバックパケットを、もし必要ならば、直ちにパーズし、暗号処理する段階と、

もし顧客インタフェースが使用不能であればループバックパケットを記憶する段階とをも具備する請求項5に記載の方法。

【請求項7】　パケットを顧客インタフェースへ送信するのに先立って、

顧客インタフェースが使用可能になる前にパケットの一部分をパーズする段階と、

パケットのパーズされた部分を先入れ先出しバッファ内に記憶して送信準備を整える段階と、

同一パケットの付加的なデータを先入れ先出しバッファ内に記憶し、該バッファから検索しながら、検索されたデータを顧客インタフェース上へ送信開始する段階とをも具備する請求項5に記載の方法。

【請求項8】　半二重顧客インタフェースから通信回路網へ送出されるデータと、通信回路網から顧客インタフェースへ到来するデータとを単一の暗号エンジンだけを使用して暗号処理する装置であって、

送出データパケットを顧客インタフェースから受信した時に、もし必要ならば、及び到来データパケットが顧客インタフェースへ送信されて来た時に、もし必要ならば、暗号処理する単一の暗号エンジンと、

到来データパケットと送出データパケットとを転送する

3

前に、必要に応じて、記憶するバッファ記憶装置手段と、
を具備し、顧客インタフェースが送出データパケットと到来データパケットとを同時に処理することができないために単一の暗号エンジンだけしか必要としないことを特徴とする装置。

【請求項9】　処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各送出データパケットをパーズする手段と、
処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各到来データパケットをパーズする手段とをも具備する請求項8に記載の装置。

【請求項10】　バッファ記憶装置手段が、
もし顧客インタフェースが使用不能であれば到来パケットを記憶する手段と、
もし通信回路網が使用不能であれば送出パケットを記憶する手段とを含む請求項9に記載の装置。

【請求項11】　顧客インタフェースが使用可能になるまで顧客インタフェースから受信したループバックパケットを記憶し、必要に応じて、暗号エンジン内において暗号処理する手段をも具備する請求項10に記載の装置。

【請求項12】　半二重顧客インタフェースから通信回路網へ送出されるデータと、通信回路網から顧客インタフェースへ到来するデータとを単一の暗号エンジンだけを使用して暗号処理する装置であって、
通信回路網から到来データパケットを受信する手段と、
顧客インタフェースが使用可能か否かを決定する手段と、
もし顧客インタフェースが使用不能であれば、各到来データパケットを記憶する手段と、
顧客インタフェースが使用可能になると作動可能になり、記憶されたデータパケットを検索する手段と、
到来データパケットを暗号処理すべきか否かを決定するためにそのデータパケットをパーズする手段と、
もし必要ならば、到来データパケットを暗号処理するように作動可能な暗号エンジンと、
到来データパケットを顧客インタフェースへ送信する手段と、
顧客インタフェースから送出データパケットを受信する段階と、
顧客インタフェースから受信した各パケットをパーズし、もし必要ならば、各パケットを処理するために暗号エンジン内へ転送する手段と、
通信回路網が使用可能であるか否かを決定する手段と、
もし通信回路網が使用不能であれば、各送出データパケットを記憶する手段と、
通信回路網が使用可能になると作動可能になり、記憶されたデータパケットを検索し、それを通信回路網へ送信する手段と、
を具備し、送出パケットの暗号処理をそれらのパケットが顧客インタフェースから受信した時に遂行し、また到来パケットの処理をそれらのパケットが顧客インタフェースへ送信する時に処理するが、顧客インタフェースの半二重動作がこれらの両機能の同時発生の可能性を妨げるためにデータの暗号処理を遂行するには単一の暗号エンジンで十分であることを特徴とする装置。

4

【請求項13】　ループバックデータパケットを記憶する手段をも具備し、送出パケットを受信しパーズする手段が、ループバックパケットを顧客インタフェースから受信するとこれらのループバックパケットを受信しパーズするようにも働き、また暗号エンジンが、必要に応じて、ループバックパケットを暗号処理するようにも働く請求項12に記載の装置。

【請求項14】　データパケットを記憶する手段に対する双方向アクセスを提供する高速データバスをも具備する請求項13に記載の装置。

【請求項15】　到来データパケットの一部分を、顧客インタフェースへ送信する前に記憶する先入れ先出しバッファと、
顧客インタフェースが使用可能になる前に先入れ先出しバッファ内に記憶されているパケットの一部分のパージングを開始して送信準備を整える手段と、
顧客インタフェースが使用可能になると先入れ先出しバッファからデータを検索し、同一パケットの付加的なデータを先入れ先出しバッファ内に記憶し、該バッファから検索しながら、検索されたデータの顧客インタフェース上への送信を開始する手段とをも具備する請求項12に記載の装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、一般的には通信回路網における暗号処理に関する。具体的には、通常は比較的ローカルなコンピュータ及び他の装置の回路網であるユーザまたは“顧客”インタフェースと、選択された宛先へ顧客インタフェースからメッセージを伝送する通信回路網との間に配置される暗号装置に関する。

【0002】

【従来の技術】多くの他のシステム及び顧客が通信回路網への合法的なアクセスを有しているから、これらの伝送の安全性が屡々重要な問題となる。異なる回路網プロトコル層における動作のための種々の通信安全プロトコルが開発されている。これらの安全プロトコルの本質の詳細は、どのような所望の安全プロトコルを取り扱うこともできる本発明にとっては重要ではない。

【0003】本発明が関係する安全サービスの原理的な型は、機密性のための暗号と、完全性のための暗号とを含む。機密性とは、発信者から無許可の個人または構成要素へ情報が伝送されないように保護することである。

5

この目的のために、情報は伝送される前に暗号化された形状に変換され、宛先において受信されると“解読された本文”形状に解読される。完全性とは、受信したデータが伝送中に変更されたか否かを検出することを含む。この目的のためには情報を暗号化する必要はなく、単に伝送経路の各端において独特な暗号検査合計を発生させるような処理を行うに過ぎない。もし検査合計が整合しなければ、当該データは変更されたものと見做される。

【０００４】理想的には、暗号処理はユーザまたは顧客に対して“透明”にすべきである。そのようにすればメッセージの送受信を、暗号処理の性質に、またはその存在にさえ関係することなく遂行することができ、その使用が“待ち時間”と呼ばれる伝送遅延時間を大幅に増大させたり、または“処理能力”即ち顧客と回路網との間のデータの流れのレートに重大な影響を与えたりすることははなくなる。しかしながら完全に透明な暗号処理は複雑でもあり、また費用もかかる。従って、顧客インタフェースに接続されている各関連装置が暗号処理のある面に対する責を負っているような費用のかからない非透明暗号処理技術が要望されている。

【０００５】回路網に使用する暗号システムを設計する場合の重要な目標は、データパケットが何れの方向に通過しようとも重大な遅延をもたらさない“オンザフライ”で処理を遂行できるように、暗号処理を顧客インタフェースと通信回路網との間に配置すべきことである。若干の形態においては暗号処理を顧客インタフェース制御装置内に組み入れることができるが、それでも暗号処理は通信経路において遂行される。データは、暗号装置を通して両方向に伝送しなければならないから、殆どの従来装置は両方向のデータ流を同時に処理するために２つの独立暗号エンジンを使用していた。単一の暗号エンジンを使用すると一方向の、まはた他の方向の処理に遅延を生じさせることによって性能に悪影響を与えるものと広く信じられている。

【０００６】従って、回路網通信の暗号処理の分野における改善が未だに要望され、特に、従来装置の性能を低下させないような低価格装置、即ち単一の暗号エンジンだけしか必要としない装置が要望されている。本発明はこの要望を満足させるものである。

【０００７】

【発明の概要】本発明は、単一の暗号エンジンだけを使用するが、２つの暗号エンジンを使用する装置に比して通信の処理能力または待ち時間に何等の悪影響をもたらさない暗号インタフェースを通信回路網と半二重顧客インタフェースとの間に設けた暗号処理装置、及び関連する方法を提供する。要約すれば、そして一般的に表現すれば本発明の方法は、送出されるデータパケットを顧客インタフェースから受信した時に、もし必要ならば、唯一の暗号エンジンを使用して暗号処理する段階と、到来データパケットが顧客インタフェースへ送信されて来た

6

時に、もし必要ならば、上記唯一の暗号エンジンを使用して暗号処理する段階と、到来データパケットと送出データパケットとを転送する前に、必要に応じて、一時バッファ記憶装置内に記憶する段階とからなる。殆どの場合には、データパケットは“カットスルー”動作と呼ばれる動作で直ちに転送されよう。顧客インタフェースが送出パケットと到来パケットとを同時に処理することができないために、単一の暗号エンジンだけしか必要としない。

【０００８】本方法は、処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各送出データパケットをパーズ（または構文解析）する段階と、処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各到来データパケットをパーズする段階とをも含むことが好ましい。到来パケットと送出パケットとを一時バッファ記憶装置内に記憶する段階は、もし顧客インタフェースが使用不能であれば到来パケットを記憶する段階と、もし通信回路網が使用不能であれば送出パケットを記憶する段階とを含む。

【０００９】本発明の方法は、ループバックパケットを顧客インタフェースから受信する段階と、ループバックパケットを、もし必要ならば、直ちにパーズし、暗号処理する段階と、もし顧客インタフェースが使用不能であればループバックパケットをループバックバッファ記憶装置内に記憶する段階とをも含むことができる。以下に説明するように、本発明の好ましい実施例は、　通信回路網から到来するデータパケットを受信する段階と、顧客インタフェースが使用可能か否かを決定する段階と、使用不能であれば、到来各データパケットを到来バッファ記憶装置内に記憶する段階を含む。次いで顧客インタフェースが使用可能になると、本方法は記憶されたデータパケットを検索する段階を含む。これに続くのは、データパケットを暗号処理すべきか否かを決定するためにパーズし、もし必要ならば、パケットを暗号処理し、そのパケットを顧客インタフェースへ送信する段階である。他方向におけるトラフィックに対しては本方法は、顧客インタフェースから送出されるデータパケットを受信する段階と、顧客インタフェースから受信した各パケットをパーズする段階と、もし処理が必要であると決定されれていれば、顧客インタフェースから受信した各パケットを暗号処理する段階と、通信回路網が使用可能であるか否かを決定する段階とを含む。もし通信回路網が使用不能であれば本方法は、各送出されるデータパケットを記憶する段階と、回路網が使用可能になるとデータパケットを検索する段階を含む。本方法の最終段階は、送出されるパケットを通信回路網上に送信することである。

【００１０】送出パケットを顧客インタフェースから受信した時に送出パケットの暗号処理が遂行され、また到

7

来パケットを顧客インタフェースへ送信する時に到来パケットの暗号処理が遂行されるので、データの両暗号処理段階を遂行するには単一の暗号エンジンで十分である。顧客インタフェースの半二重動作が、これらの両機構を同時に要求する可能性を妨げる。

【００１１】ループバックパケットを処理することに関して本方法は、ループバックパケットを顧客インタフェースから受信する段階と、ループバックパケットを、もし必要ならば、直ちにパーズし、暗号処理する段階と、もし顧客インタフェースが使用不能であればループバックパケットを記憶する段階とを含む。本発明の別の面によれば、方法は更に、顧客インタフェースが使用可能になる前に到来データパケットの一部分をパーズする段階と、パケットのパーズされた部分を先入れ先出しバッファ内に記憶して送信準備を整える段階と、顧客インタフェースが使用可能になると先入れ先出しバッファからデータを検索する段階と、同一パケットの付加的なデータを先入れ先出しバッファ内に記憶し、該バッファから検索しながら、検索されたデータを顧客インタフェース上へ送信開始する段階とをも含む。先入れ先出しバッファを使用することによって、インタフェースが使用可能になった直後に、遅延を伴わずに顧客インタフェース上への送信が開始されるようになる。

【００１２】新しい装置に関しては本発明は、その最も広義の表現では、送出データパケットを顧客インタフェースから受信した時に、もし必要ならば、及び到来データパケットが顧客インタフェースへ送信されて来た時に、もし必要ならば、暗号処理する単一の暗号エンジンと、到来データパケット及び送出データパケットを転送する前に、必要に応じて、記憶するバッファ記憶装置手段とを含む。前述のように、顧客インタフェースが送出データパケットと到来データパケットとを同時に処理することができないから、この目的のためには単一の暗号エンジンで十分である。本発明の装置は、ループバックデータパケットを記憶する手段をも含むことができ、また上述した種々の形状を有する本発明の方法の範囲に対比できる他のより特定の表現によって限定することもできる。

【００１３】以上の説明から、本発明が回路網通信に使用するための暗号処理の分野に重要な進歩をもたらしていることが明白になったであろう。即ち本発明は、単一の暗号エンジンを使用しながら２つの暗号エンジンを使用する装置に比して処理能力または待ち時間を何等劣化させることなく、通信回路網と顧客インタフェースとの間の双方向暗号処理を提供する。

【００１４】以下に添付図面に基づいて本発明の好ましい実施例を説明するが、この説明から本発明がより明白になるであろう。

【００１５】

【実施例】例として添付図面に示すように、本発明は顧

8

客インタフェースと通信回路網との間を両方向に通過するデータパケットを暗号処理する装置に関する。従来は、最小の遅延で両方向のトラフィックを効率的に処理するためには、少なくとも２つの独立的に作動する暗号エンジンを含む必要があるものと考えられていた。本発明以前には、単一の暗号エンジンを使用すると必然的に待ち時間または処理能力にある種の性能低下がもたらされるものと考えられて来た。

【００１６】本発明によれば、装置の待ち時間または処理能力に重大な影響を与えることなく、顧客インタフェースと通信回路網との間で両方向の暗号処理をするために単一の暗号エンジンを使用する。この目標を単一の暗号エンジンを用いて達成することは不可能に見えるかも知れないが、もし顧客インタフェース内の通信媒体へのアクセスのために使用されるプロトコルが、一般にキャリア検知多重アクセス／衝突検出（ＣＳＭＡ／ＣＤ）と呼ばれるプロトコルを使用するイーサネットのような半二重媒体であれば、可能である。回路網バスまたはケーブルへのアクセスのためのＣＳＭＡ／ＣＤ規約の下では、送信を望んでいるどのステーションも、送信を開始する前にそのケーブルが話し中でないことを確認するために先ず“聴守”しなければならない。回路網上の全てのステーションは平等のアクセス優先順位を有しており、ラインが話し中でなくなると直ちに、そして何等のパケット間遅延も要求されることなく送信を開始することができる。しかしながら、もし送信を開始した第１のステーションが別のステーションからの送信との“衝突”を検出すれば、第１のステーションは短い時間の間にわたって送信を継続し、送信を望んでいる全ステーションに衝突を検出させる。次いで第１のステーションはランダムな時間の後に送信を終了する。衝突に関与している他のステーションは同じことはせず、送信の再開を試みる前にランダムな、従って通常は異なる遅延時間を選択する。

【００１７】回路網アクセスに関するＣＳＭＡ／ＣＤ規約は、全二重伝送を、即ち同時に送受信することを許容しないようになっている。もしあるステーションがメッセージを受信中であれば回路網は話し中であり、このステーションまたは他のどのステーションからも送信を開始することはできない。同様に、もしこのステーションから送信が進行中であれば、このステーションがメッセージを送っている間は他のステーションは回路網にアクセスを得ることはできないので、同時にメッセージを受信することはできない。従って、イーサネットまたは他のＣＳＭＡ／ＣＤステーションの動作の性質は半二重、即ちメッセージの送信及び受信の両方を同時に行うことはできないが、回路網アクセス規約の性質から、同時でなければ可能である。イーサネット及びＣＳＭＡ／ＣＤのこの特性が本発明に、特定的には顧客インタフェース内に使用され、単一の暗号エンジンを通して、２つの暗

9

号エンジンを使用する装置に比して待ち時間または処理能力に何等の劣化を与えることなく、メッセージの双方向伝送を提供する。しかしながら、本発明はＣＳＭＡ／ＣＤとの併用に限定されるものではなく、どのような半二重通信媒体とも同じように動作することは明白である。

【００１８】図１は顧客インタフェース１０と通信回路網１２との間に接続されている実施例の装置を簡易ブロック線図で示している。以下の説明では、顧客インタフェースに関連する装置の面を装置の“顧客側”と呼ぶことがあり、また通信回路網に関連する装置の面を装置の“回路網側”と呼ぶことがある。装置の関連成分は、顧客受信装置（ＲｘＣ）１４、顧客送信装置（ＴｘＣ）１６、回路網受信装置（ＲｘＮ）１８、回路網送信装置（ＴｘＮ）２０、単一の暗号エンジン２２、バッファ記憶装置２４、顧客送信ＦＩＦＯ記憶装置２６、受信パーザ２８及び送信パーザ３０を含む。

【００１９】これらの成分は、特定の時点に処理するトラフィックの型に依存して種々の論理構成に接続される。説明する全ての経路はバッファ記憶装置２４を通過しているが、バッファ記憶装置をデータパケット記憶装置としてではなく、各データ経路の一部として使用する２つの直接論理経路が存在する。第１に、顧客インタフェース１０から回路網ケーブル１２までの直接論理経路が存在する。この経路は顧客インタフェース１０から顧客受信装置１４までの線３２と、顧客受信装置から（バッファ記憶装置２４を介して）回路網送信装置２０までの線３４と、回路網送信装置から回路網ケーブル１２までの第３の線３６とを含む。同様に、通信回路網１２から顧客インタフェース１０までの別の直接論理経路は、通信回路網から回路網受信装置１８までの線３８と、回路網受信装置から（バッファ記憶装置２４を介して）顧客送信ＦＩＦＯ記憶装置２６までの線４０と、ＦＩＦＯ記憶装置から顧客送信装置１６までの別の線４２と、顧客送信装置から顧客インタフェース１０までのさらなる線４４とを含む。実際には論理的に分離している３つの記憶装置であるバッファ記憶装置２４は、データバス４６によって、線３４に沿う“送出”データ経路と、線４０に沿う“到来”データ経路とに接続されている。

【００２０】以上のデータ経路の説明からバッファ記憶装置２４は、データパケットを直ちに送信できない場合にはそれらを記憶するように働き、また全パケットを記憶することなくデータを直ちに転送するようにも働くことが理解されよう。これらの両動作は、技術的には記憶装置内にデータを“記憶”することを含むが、この説明では“記憶”すると言う語は全データパケットが爾後に通信回路網または顧客インタフェース上へ転送するために保持するような状況のために保留する。“カットスルー”動作モードにおいてデータパケットがバッファ記憶装置を通過する場合には、あるパケットの一部分がまだ

10

記憶装置に到着しつつある間にもそのパケットは既に記憶装置から送信されている。

【００２１】双方向トラフィックの見掛け上の同時処理に対する鍵は、図２のデータ流れ図を参照すると理解し易い。顧客インタフェース１０から受信されるデータパケットは、それが受信されると受信パーザ２８によって必ずパーズされ、受信パーザ２８内におけるパージング処理から暗号処理が必要であることが決定されると、エンジン２２によって暗号処理される。次いで暗号処理がなされている、いないに拘わらず、データパケットは、通信回路網１２へのアクセスを待機する必要がある限りバッファ記憶装置２４内に記憶される。これに対して、通信回路網１２から受信したデータパケットは直ちにパーズまたは暗号処理されることなく、先ず一時的に記憶するためにバッファ記憶装置２４に導かれる。通常は、顧客インタフェースは使用可能であり、パケットは直ちにバッファ記憶装から検索されよう。実際に通常はパケットは、それがまだ通信回路網１２から受信中でも顧客インタフェースへ送信されることになろう。これは、もし顧客インタフェースが使用不能であれば全パケットを一時記憶装置内に保持する“蓄積転送”動作に対して、“カットスルー”動作として知られている。何れの場合も、顧客インタフェースが使用可能であるか、または後刻使用可能になれば、パケットはバッファ記憶装２４から送給され、送信パーザ３０によってパーズされ、もし必要ならばエンジン２２によって暗号処理され、そして最後に顧客インタフェース１０へ転送される。暗号エンジン２２は、使用することが要求されると、顧客インタフェース１０から受信されているデータパケットを処理するか、または顧客インタフェース１０へ送信されて来たデータパケットを処理するの何れかを遂行する。もし顧客インタフェースが既に話し中でデータパケットを装置へ送給していれば送出パケットのパージング及び考え得る暗号処理は開始されないから、エンジン２２のこれら２つの機能が同時に要求されることはあり得ない。

【００２２】詳述すれば、回路網受信装置１８によって通信回路網１２から受信されたデータパケットは直接バッファ記憶装置２４へ転送される。もし顧客インタフェース１０が現在パケットを送信または受信していなければ、そのパケットは顧客送信ＦＩＦＯ記憶装置２６に転送され、また並列に送信パーザ３０によってパーズされる。もし必要ならば、パーザによって決定された適切なバイトから、データは顧客送信ＦＩＦＯ記憶装置２６に転送される前に暗号エンジン２２を通過させられる。最後に、顧客送信装置１６はデータを顧客送信ＦＩＦＯ記憶装置２６から引き出し、データパケットを顧客インタフェース１０へ送信する。

【００２３】通信回路網１２から受信されたパケットがバッファ記憶装置２４へ入った場合には、もし現在パケットを顧客インタフェース１０から受信してはいるが、

顧客インタフェースへ送信すべき未処理パケットが存在していなければ、そのパケットの始めの部分は、あたかもそれが送信されるもののように顧客送信ＦＩＦＯ記憶装置２６へ転送され、その始めの部分のパージングが遂行される。しかし、顧客インタフェースはまだ話し中であると見られるから暗号処理が開始されることはなく、また顧客送信装置１６が顧客送信ＦＩＦＯ記憶装置２６からデータを引き出すこともない。顧客送信ＦＩＦＯ記憶装置２６が一杯になると、実際の送信が開始され顧客送信装置１６が顧客送信ＦＩＦＯ記憶装置２６からデータを引き出し始めるまで、それ以上のデータは転送されない。ＦＩＦＯ記憶装置のこのプリローディングは、暗号エンジン２２が動作し始める時に、そしてそれがデータの第１ブロックを処理し、エンジンのデータの“パイプライン”が安定状態に達するまで、データの“アンダーラン”が送信されないようにする。

【００２４】図３は、本発明の装置をより詳細に示す図である。図３には示されているが、図１及び２の簡易図には示されていない成分は、バッファ記憶装置２４を制御する記憶装置制御装置５０と、顧客受信制御論理回路（ＣＲＣＴＬ）５２と、顧客送信制御論理回路（ＣＴＣＴＬ）５４と、パケット制御論理回路５６と、４つの直接メモリアクセスユニット（ＣＲＤＭＡ　５７、ＮＴＤＭＡ　５８、ＣＴＤＭＡ　６０及びＮＲＤＭＡ　６２）と、３つの付加ＦＩＦＯ記憶装置（ＣＲＦＩＦＯ　６４、ＮＴＦＩＦＯ　６６及びＮＲＦＩＦＯ　６８）とを含む。これらの付加的な成分の機能について以下に概要を説明する。

【００２５】顧客受信制御論理回路（ＣＲＣＴＬ）５２は装置の顧客側の受信動作（受信パーザ２８及び暗号エンジン２２の動作の調整を含む）を制御する。顧客送信制御論理回路（ＣＴＣＴＬ）５４は、装置の顧客側の送信動作（送信パーザ３０及び暗号エンジン２２の動作の調整を含む）を制御する。付加ＦＩＦＯ記憶装置６４、６６、６８は比較的小さい記憶装置であり、その主目的はデータバス４６の効率的な動作のためのバッファとなることである。ＤＭＡユニット５７、５８、６０、６２はバッファ記憶装置２４にアクセスするための普通のＤＭＡ機能を提供する。記憶装置制御装置５０は、バッファ記憶装置の動作とデータバス４６上での関連動作とを管理する。最後に、パケット制御論理回路５６は、データの緩衝要求を最小にするように、装置の顧客側及び回路網側への、及びこれらの側からのデータ流を調整する。

【００２６】装置の顧客側から回路網側への送出データ流の場合のパージングは、パケットがデータバス４６を通してバッファ記憶装置２４へ転送されるのと同時に到来データパケットに対して（受信パーザ２８において）遂行される。パケットに対して暗号処理が要求されていることを受信パーザ２８が検出すると、パーザ２８はそ

れを顧客受信制御論理回路（ＣＲＣＴＬ）５２に通知し、顧客受信制御論理回路５２は適切な時点にデータを顧客受信装置１４から暗号エンジン２２内へ導き始める。暗号処理の後に、データパケットはバッファ記憶装置２４内に記憶される。装置の回路網側がデータパケットを受け入れ可能になると、回路網の可用性に依存して、パケット制御論理回路５６は回路網送信装置に送信を開始するように指令し、データをバッファ記憶装置２４から回路網送信装置へ、次いで通信回路網上へ転送する。カットスルーと呼ばれるこの動作は、装置の顧客側からのデータの連続受信と同時に遂行させることが可能である。

【００２７】装置の回路網側から顧客側への到来データ流は直ちにパーズされずに、回路網受信装置１８からバッファ記憶装置２４へ直接転送される。装置の顧客側が使用可能になると、パケット制御論理回路５６はパケット制御論理回路５６に指令して顧客側への転送を開始させる。この動作は回路網側からのデータの受信と同時に遂行させることが可能である。データのパケットが顧客送信ＦＩＦＯ２６へ送られ始めると、それは同時に送信パーザ３０によってパーズされる。暗号処理動作が要求されていることを送信パーザ３０が検出すると、それは顧客送信制御論理回路（ＣＴＣＴＬ）５４に通知され、顧客送信制御論理回路５４は適切な時点にデータ流を顧客受信装置１４から暗号エンジン２２内へ導き、データパケットは暗号エンジン２２から顧客送信ＦＩＦＯ２６を通って顧客インタフェースへ流れる。

【００２８】到来データパケット及び送出データパケットの他に、装置はループバックデータパケットをも処理する。ループバックデータパケットは、装置の顧客側から受信され、通常は暗号処理後に顧客側に戻されるデータのパケットである。ループバック機能によって顧客装置は、データパケットの“ローカル”暗号処理が可能になる。ループバック動作は、ファイル暗号文のような暗号サービスを顧客に提供する。ループバック機能は、例えばもし到来データパケットが、遂行されるべきではない時点に偶発的に解読されるか、または到来パケットを解読すべきであるのに解読されていない場合にも必要である。基本的には、ループバック機能は送出パケットではないデータパケットの暗号処理へのアクセスを顧客に与える。装置の顧客側から受信したループバックパケットは、送出パケットと殆ど同じようにして処理される。それらはバッファ記憶装置２４への途上でパーズされるが、送出バッファの代わりに、バッファ記憶装置のループバックバッファ内に記憶される。ループバックパケットを顧客に送り返す時点、即ち顧客側が使用可能でありループバックパケットを送信する転機である時点になると、パケットは何等の付加的な処理も受けずに顧客に直接送り返される。

【００２９】受信パーザ２８及び送信パーザ３０におい

て遂行される特定のパージング手順は、回路網プロトコル及び使用する特定のデータパケットフォーマットに大きく依存し、本発明の一部であるとは考えていない。パージングは、あるデータパケットに対して暗号処理が必要か否かを決定するために、単にそのパケット内の見出し情報を走査するに過ぎない。顧客装置は、暗号処理を要求するのか否かを見出し内に指示することを要求される。暗号処理を要求していることを指示している見出しフィールドを受信パーザ２８が検出すると、データパケットは適切な部分が暗号エンジン２２を通るように進路変更される。パーザ２８は１以上の異なるパケットフォーマットを認識し、各フォーマット内の暗号処理を要求していることを指示するコードを検出するように設計することができる。パージングは、パケット内の暗号処理を開始すべき開始点の決定をも含む。暗号処理は、例えばデータ暗号化標準によるデータフレームの指定された部分の暗号化、またはデータパケットに追加するために完全性検査値（ＩＣＶ）と呼ばれるフレーム検査シーケンス（または検査合計）の計算、または両者を含む。

【００３０】送信パーザ３０は、回路網側から到来するどのパケットを暗号処理するのかを決定する。この場合もパージング機能は、フレーム見出し情報を走査し、この見出し情報に基づいて決定を行うのである。もしある到来パケットに対して暗号処理が要求されていれば、そのパケットの適切な部分が暗号エンジン２２に向けられる。通常、到来パケットの処理は解読、または単にデータの完全性を保証するためのフレーム検査シーケンスの再計算を含む。

【００３１】以上の説明から、本発明が回路網通信の暗号処理の分野に重要な前進を提供していることが理解されたであろう。具体的には、本発明は単一の暗号エンジンを使用してはいるが付加的な待ち時間を導入することなく、また処理能力に影響を与えることなく、回路網と

顧客装置との間に転送されるメッセージトラフィックの暗号処理に、複雑さを逓減させた手法を提供しているのである。例示の目的から、本発明の実施例の詳細を説明したが、本発明の思想及び範囲から逸脱することなく種々の変更を施すことができよう。従って、本発明は特許請求の範囲を除いて上記説明に限定されるものではないことを理解されたい。

【図面の簡単な説明】

【図１】顧客インタフェースと通信回路網との間に接続され、単一の暗号エンジンだけを有する本発明の実施例の暗号装置のブロック線図。

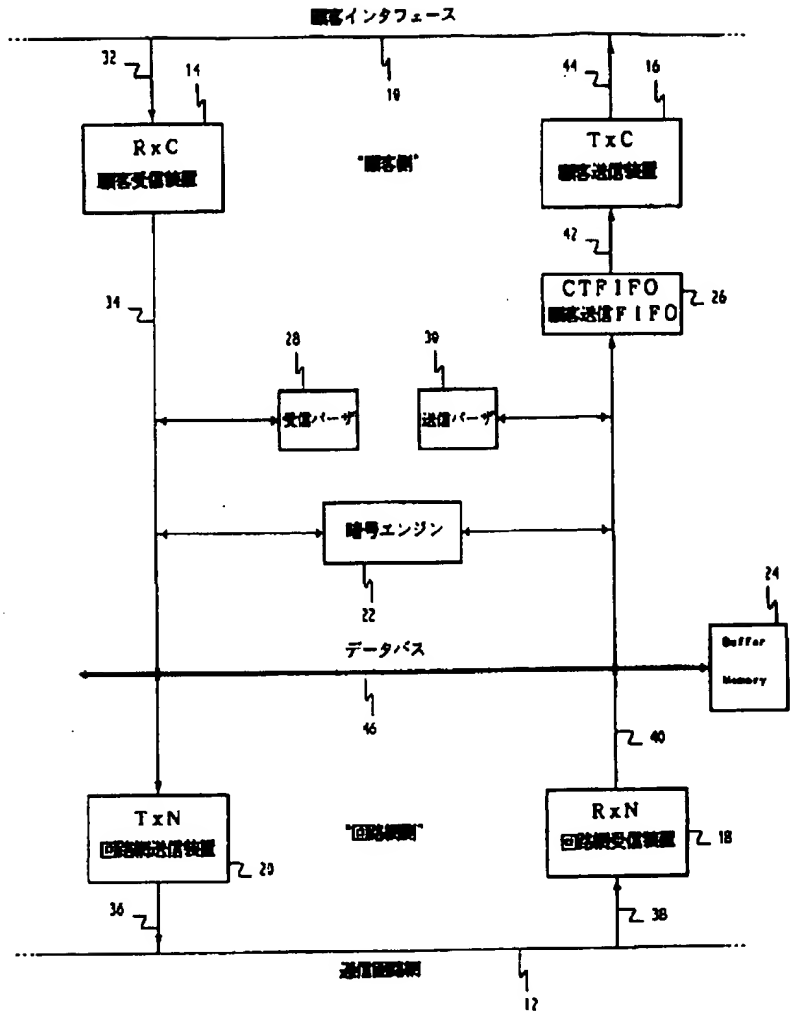
【図２】図１に類似した簡易化ブロック線図。

【図３】図１及び２に類似したより詳細なブロック線図。

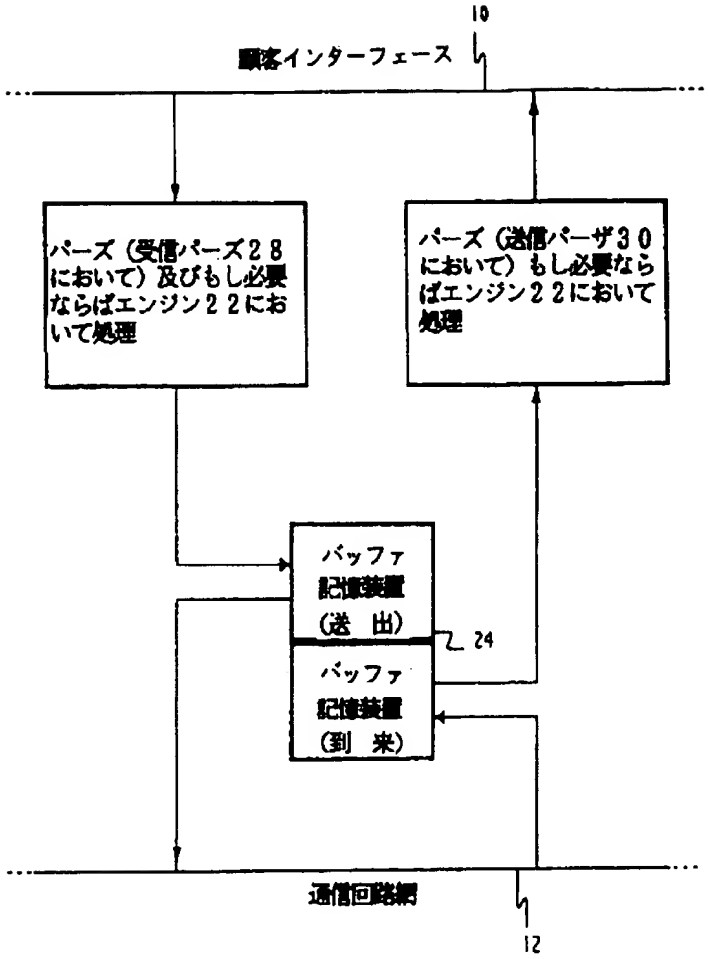
【符号の説明】

１０　顧客インタフェース
１２　通信回路網
１４　顧客受信装置
１６　顧客送信装置
１８　回路網受信装置
２０　回路網送信装置
２２　暗号エンジン
２４　バッファ記憶装置
２６　顧客送信ＦＩＦＯ記憶装置
２８　受信パーザ
３０　送信パーザ
４６　データバス
５０　記憶装置制御装置
５２　顧客受信制御論理回路
５４　顧客送信制御論理回路
５６　パケット制御論理回路
５７、５８、６０、６２　直接メモリアクセスユニット
６４、６６、６８　付加ＦＩＦＯ記憶装置

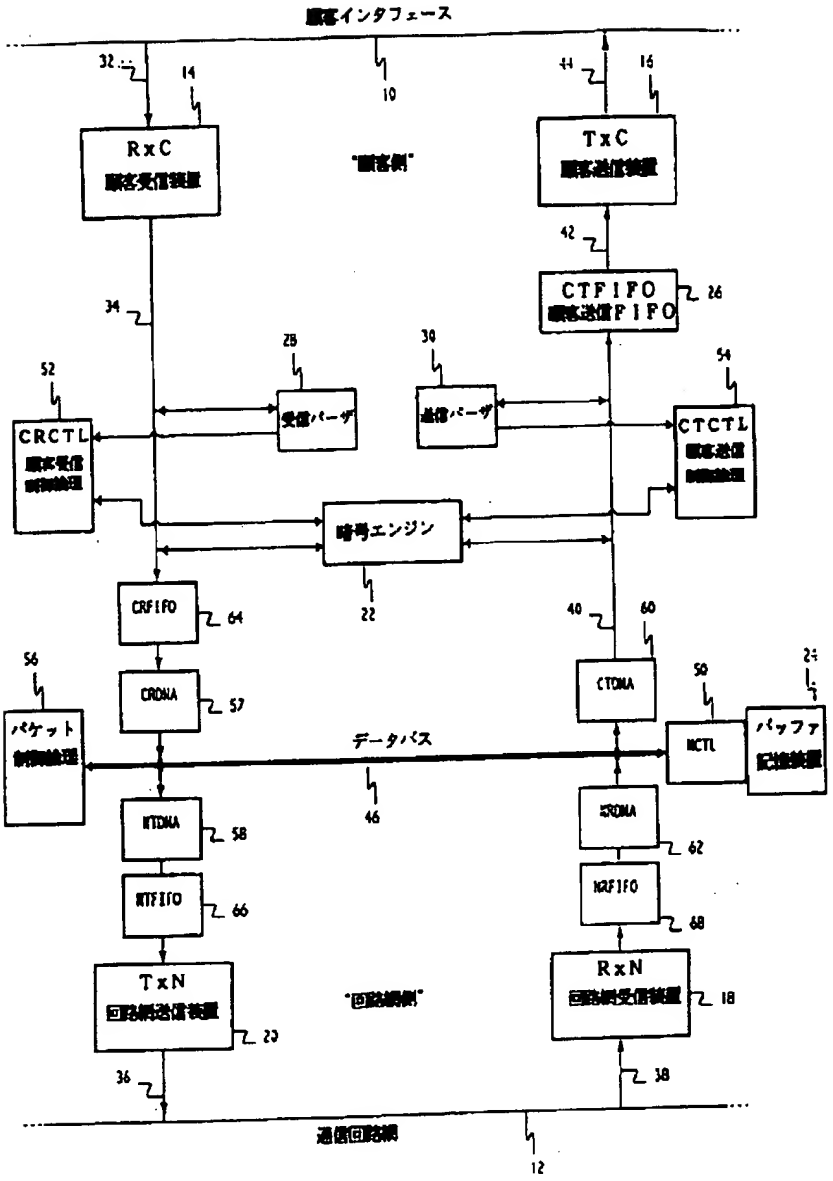
【図1】


顧客インタフェース
32
14
10
44
16
RxC
顧客受信装置
"顧客側"
TxC
顧客送信装置
42
CTFIFO
顧客送信FIFO
26
34
28
30
受信バーザ
送信バーザ
暗号エンジン
22
24
データバス
Buffer
Memory
46
40
TxN
回線網送信装置
29
"回線網側"
RxN
回線網受信装置
18
36
38
通信回線網
12

【図2】


10
顧客インターフェース
パーズ（受信パーズ28において）及びもし必要ならばエンジン22において処理
パーズ（送信パーザ30において）もし必要ならばエンジン22において処理
バッファ記憶装置（送 出）
24
バッファ記憶装置（到 来）
通信回路網
12

【図3】


顧客インタフェース
32
14
10
44
16
RxC
顧客受信装置
"顧客側"
TxC
顧客送信装置
42
CTFIFO
顧客送信FIFO
26
34
28
30
54
52
CRCTL
受信パーザ
送信パーザ
CTCTL
暗号エンジン
22
CRFIFO
64
40
60
56
CRDMA
57
CTDMA
50
24
パケット
データバス
MCTL
バッファ
46
NTDMA
58
NRDMA
62
NTFIFO
66
NRFIFO
68
TxN
"回線網側"
RxN
18
20
36
38
通信回線網
12